

GEMMA Gegevenslandschap

Beschrijving informatiearchitectuur

Leeswijzer

Dit document beschrijft de visie van VNG Realisatie ten aanzien van een nieuwe, flexibele en generieke gemeentelijke informatiearchitectuur geschetst: het GEMMA Gegevenslandschap.

Dit document is bestemd voor informatiemanagers, adviseurs en architecten.

Het document is als volgt opgebouwd:

- Hoofdstuk 1 beschrijft het GEMMA Gegevenslandschap op hoofdlijnen;
- Hoofdstuk 2 beschrijft de uitwerking van functies van het GEMMA Gegevenslandschap.

Dit document is in beheer bij VNG-Realisatie.

Tabel 1. Documenthistorie

Versie	Toelichting	Datum	Opsteller(s)
1.0	Goedgekeurde versie door squad architectuur	november 2018	VNG Realisatie
1.1	Aanpassingen aan hoofdstuk Uitwerking GEMMA Gegevenslandschap	april 2019	VNG Realisatie
1.11	Aanpassingen aan hoofdstuk Inleiding	juni 2019	VNG Realisatie
1.20	Aanpassingen n.a.v. consultatie met gemeenten en leveranciers	oktober 2019	VNG Realisatie

Inhoudsopgave

GEMMA GEGEVENS LANDSCHAP	1
Leeswijzer	2
Inhoudsopgave	3
1. GEMMA Gegevenslandschap	5
1.1. Organisatorisch werkingsgebied	6
1.2. Functioneel werkingsgebied	6
1.3. Scheiding van rollen	7
1.4. Bevraging bij de bron	11
1.5. Authenticatie en autorisatie	12
1.6. Open en gesloten gegevens	13
1.7. Doelbinding voor gegevensverwerking	13
1.8. Privacy en security	14
1.9. Standaardisatie via informatiemodellen	15
1.10. Standaardisatie van gegevensontsluiting	16
1.11. Standaardisatie van processen	17
1.12. Aansluiting op de GEMMA informatiearchitectuur	17
2. Uitwerking GEMMA Gegevenslandschap	19
2.1. Interactie	20
2.1.1. Procesondersteuning	20
2.1.2. Regie op gegevens	20
2.1.3. Aanvragen en meldingen	21
2.1.4. Eindgebruiker authenticatie	21
2.2. Procesinrichting	22
2.2.1. Procesinrichting en uitvoering	23
2.2.2. Bedrijfsregels	23
2.2.3. Data analyse ondersteuning	23
2.2.4. Functie autorisatie	24
2.2.5. Doel en grondslag	24
2.2.6. Audit logging	25
2.3. Integratiefuncties	26
2.3.1. Netwerk	26
2.3.2. Netwerkbeveiliging	26
2.3.3. Verbinden	27
2.3.4. Dienstencatalogus	27
2.4. Diensten	28
2.4.1. Organisatie authenticatie	28

2.4.2. Diensten autorisatie	29
2.4.3. Diensten	29
2.4.4. Terugmelden	30
2.4.5. Abonneren en notificeren	31
2.4.6. Audit logging.....	32
2.4.7. Transformatie	32
2.4.8. Integratie	32
2.4.9. Pseudonimisering en anonimisering	33
2.5. Gegevensbronnen	34
2.5.1. Bijhouding gegevens.....	34
2.5.2. Historie en metadatering gegevens	35
2.5.3. Protocollering	35

1. GEMMA

Gegevenslandschap

Het huidige gemeentelijk gegevenslandschap biedt onvoldoende mogelijkheden om de ambities van gemeenten op het vlak van het ondersteunen van burgers, bedrijven en de interne organisatie te realiseren.¹ Processen die gebruik maken van gegevens zijn slechts beperkt gestandaardiseerd, niet afzonderlijk en autonoom aan te spreken of uit te voeren en niet eenduidig en onweerlegbaar vastgelegd. Gegevens die worden gebruikt vanuit processen zijn daarnaast beperkt gestandaardiseerd waardoor de portabiliteit van gegevens beperkt is. Daarnaast vergt het voldoen aan onder andere privacy- en informatiebeveiliging wet- en regelgeving met huidige inrichting veel inspanning van gemeenten. Een andere inrichting van het gegevenslandschap is nodig om gemeenten in staat te stellen om hun taken op een effectieve en efficiënte wijze uit te voeren. Belangrijke doelen die met de nieuwe inrichting worden nagestreefd zijn:

- Gemeenten de regie geven over de eigen gegevens;
- Verhogen van de portabiliteit van gegevens;
- Interne en externe transparantie over de verwerking van gegevens;
- De burger zeggenschap geven over de 'eigen' gegevens;
- Eenvoudig kunnen voldoen aan vigerende wetgeving onder andere op het gebied van informatiebeveiliging en bescherming van de privacy;
- Stimuleren van innovatie van eindgebruikerstoepassingen.

Gemeenten moeten kunnen groeien naar een situatie waarin burgers effectief en efficiënt worden gefaciliteerd in hun rechten. Daarnaast moet de gemeente zowel voor interne als externe transparantie op eenvoudige, en liefst geautomatiseerde wijze, inzage kunnen geven welke medewerker of rol, op welk moment toegang heeft gehad tot vertrouwelijke gegevens of deze heeft bewerkt. Om dit te kunnen realiseren worden de onderstaande aantal principes nagestreefd.

- Werken met componenten die afgebakende functionaliteit kennen en via gestandaardiseerde interfaces communiceren. Een hierop gebaseerd informatielandschap stelt gemeenten in staat om wendbaar en innovatief te opereren omdat wijziging of vervanging per component mogelijk wordt;
- Maximaal open stellen van gegevens voor hergebruik. Het delen en gebruiken van gegevens wordt slechts beperkt door wetgeving en niet door ideeën over het gebruik van gegevens. Door als overheid open te zijn waar dit kan, wordt de informatiepositie van klanten versterkt, wordt publiek/private samenwerking gefaciliteerd en neemt het vertrouwen in de overheid toe;

¹ Zie "Gegevenslandschap - Aanleiding vernieuwing gemeentelijke informatievoorziening" (<http://www.gemmaonline/...>)

- Zorg dragen voor een goede beveiliging van gegevens en garanderen van de bescherming van de privacy. Om invulling te kunnen geven aan zowel verwachtingen van de burger als de wettelijke vereisten realiseren we een samenhangend geheel van technische, organisatorische, fysieke en procedurele maatregelen;
- Eenmalige inwinnen en vastlegging van gegevens en voorkomen van kopieën van brongegevens. Brongegevens worden alleen bewerkt bij de bron en komen via diensten beschikbaar voor processen die ze nodig hebben;
- Faciliteren van persoonlijk datamanagement voor partijen die daartoe gerechtigd zijn. Persoonlijk datamanagement draagt bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen;
- Standaardisatie op alle gebieden waar dit meerwaarde levert door het maken van afspraken en standaarden. Afspraken en standaarden zijn nodig om effectief, efficiënt en veilig samen te werken en informatie uit te wisselen. Ze zijn ook nodig om voldoende onafhankelijk te blijven en de juiste samenwerkingspartners te kunnen kiezen.

Toepassing van het bovenstaande krijgen gemeenten grip op de gegevenshuishouding waardoor ze wendbaarder kunnen opereren en daardoor effectievere dienstverlening kunnen leveren aan burgers en bedrijven. Verantwoording afleggen over de verwerking van gegevens en de redenen van verwerking zowel naar bestuur als naar afnemers wordt hierdoor eenvoudiger. Gemeenten worden daardoor in staat gesteld om op een eenvoudigere manier compliant aan wet- en regelgeving te werken.

1.1. Organisatorisch werkingsgebied

Het GEMMA Gegevenslandschap is de architectuur die wordt gebruikt binnen op realisatie gerichte projecten zoals Common Ground. Het organisatorisch werkingsgebied voor het GEMMA Gegevenslandschap is primair gemeenten en gemeentelijke samenwerkingsverbanden. Het staat andere overheidslagen en bevoegd gezagen uiteraard vrij om gebruik maken van dit architectuurmodel.

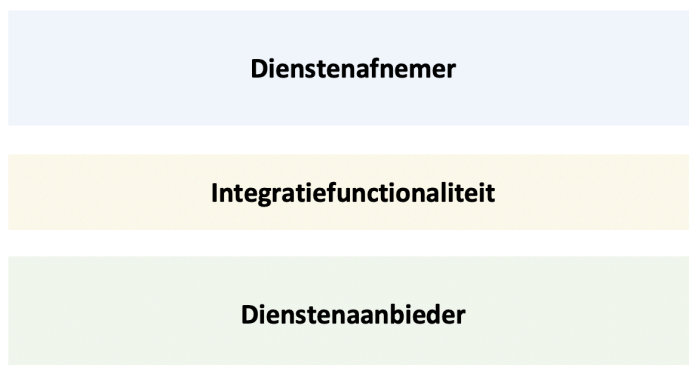
1.2. Functioneel werkingsgebied

Het GEMMA Gegevenslandschap is primair gericht op transactionele dienstverlening. Het is geen model voor bijvoorbeeld streaming datadiensten zoals VoIP of streaming sensordata. Voor ondersteuning van data-gedreven werken en business intelligence biedt het model van het gegevenslandschap aanknopingspunten, maar voor met name business intelligence en data-intensieve bewerkingen moet onderzocht worden in hoeverre de geschetste architectuur werkbaar is, en onder welke voorwaarden dit het geval is.

De bestaande GEMMA biedt een referentie-beschrijving van het proces- en informatielandschap van gemeenten (referentiecomponenten, bedrijfsfuncties, applicatiefuncties, processenlandschap,...). Het GEMMA Gegevenslandschap richt zich meer op het 'hoe' door in samenhang benodigde functionaliteiten te beschrijven

1.3. Scheiding van rollen

De voorgaande paragraaf beschrijft de kern van de vernieuwde inrichting van het GEMMA Gegevenslandschap, namelijk het scheiden van processen en gegevens en wijziging van de verantwoordelijkheden ten aanzien van de wijze van modellering en ontsluiting van gegevens. In de nieuwe inrichting worden een aantal rollen onderscheiden; leveranciers van diensten (dienstenaanbieders) en afnemers van diensten (dienstenaanbieders). Dienstenaanbieders maken voor het afnemen van diensten van dienstenaanbieders gebruik van een integratiefaciliteit.



Figuur 1 – Rollen van het gegevenslandschap

Dienstenaanbieder – een dienstenaanbieder levert de gebruikersinterfaces en procesinrichting voor medewerkers van de gemeente en burgers en bedrijven. De gebruikersinterfaces kunnen bijvoorbeeld de vorm hebben van een mobiele app, website of traditionele procesapplicatie. De gebruikersinterfaces maken gebruik van bedrijfsregels bij de uitvoering van processen. Voor het ophalen en wegschrijven van de gegevens die gebruikt worden bij de uitvoering van processen worden gestandaardiseerde diensten gebruikt. Deze diensten worden beschikbaar gesteld door dienstenaanbieders conform landelijke standaarden.

De dienstenaanbieder is verantwoordelijk voor het authenticeren en autoriseren van eindgebruikers en borgt dat alleen geautoriseerde gebruikers gebruik kunnen maken van functies van de gebruikersinterfaces. Denk hierbij aan toepassing van DigiD en eHerkenning voor inwoners en ondernemers en Attribute Based Access Control (ABAC) voor het verlenen van toegang tot applicatiefuncties.

Bij het gebruik van diensten leggen zowel de dienstenaanbieder als -aanbieder vast voor welk doel en met welke wettelijke doelbindingsclaim de dienstenaanbieder de dienst gebruikt.² Deze doelbindingsclaim kan bijvoorbeeld

² Zie ook 0 -

Standaardisatie via informatiemodellen

Gemeenten nemen, met ondersteuning van VNG Realisatie, de regie over de standaardisatie van de gemeentelijke gegevens. Daar waar anno 2018 slechts een klein deel van de gemeentelijke

gegevens via informatiemodellen is gestandaardiseerd (RSGB, RGBZ, ImZTC, ImGeo en Raadsinformatie), worden in de nieuwe inrichting op termijn ook gemeentelijke kernregistraties en sectorale registraties gestandaardiseerd via informatiemodellen. Dit betekent dat nieuwe informatiemodellen ontwikkeld worden voor bijvoorbeeld het sociaal- en het belastingen domein en dat aansluiting gezocht wordt bij bestaande informatiemodellen zoals het IMBOR voor de openbare ruimte. Het is mogelijk dat binnen omvangrijke domeinen een opsplitsing naar sub-domeinen of thema's wordt gemaakt en daardoor binnen een domein meerdere informatiemodellen ontstaan. Denk hierbij bijvoorbeeld aan het sociaal domein. Dit domein omvat een groot aantal taken, waardoor opsplitsing in kleinere delen voor de hand ligt. Te denken valt dan bijvoorbeeld aan aparte informatiemodellen voor de taken die gemeenten hebben ten aanzien van de jeugdzorg, maatschappelijke ondersteuning en werk en inkomen.

Door het standaardiseren van informatiemodellen is standaardisatie van de toegang tot gegevens via diensten mogelijk. Op het moment dat vanuit dienstverlening een door gemeenten breed gedeelde behoefte aan gegevens ontstaat, kan er een standaardisatietraject starten. In dit traject wordt samen met gemeenten en marktpartijen de behoefte aan gegevens voor de betreffende processen geïnventariseerd, waarna vanuit deze behoefte een informatiemodel wordt ontwikkeld. VNG Realisatie kan regie voeren over de totstandkoming en de inhoud van de modellen. Onderdeel van het regie voeren over informatiemodellen is ook het governance model wat gehanteerd wordt. Per informatiemodel moet worden bepaald wat de meest voor de hand liggende standaardisatiepartij en bijbehorende governancestructuur is.

1.1. Standaardisatie van gegevensontsluiting

Dienstenaanbieders maken gegevens beschikbaar via diensten. Diensten doen dit bij voorkeur via een applicatie interface, ofwel Application Programming Interface (API). Een applicatie-interface is een toegangspunt waar applicatieservices beschikbaar worden gesteld. Binnen de overheid zijn afspraken gemaakt ten aanzien van de technische- en gebruiksaspecten van APIs. Deze afspraken beogen te bereiken dat binnen de overheid APIs op vergelijkbare wijze werken en beveiligd worden.

De ontwikkeling van APIs wordt afgestemd op vragen die vanuit de dienstverlening en processen worden gesteld. Hierdoor wordt geborgd dat APIs aansluiten op de behoefte die vanuit afnemers leeft. De gegevens die door de APIs worden ontsloten conformeren zich aan de gestandaardiseerde informatiemodellen. Hierdoor wordt de uitwisselbaarheid van gegevens bevorderd, en is voor alle partijen duidelijk wat de syntax, samenhang en betekenis (semantiek) van de gegevens is. Bij de ontwikkeling van diensten worden marktpartijen in een vroeg stadium betrokken, aangezien zij uiteindelijk de partijen zijn die de diensten realiseren en leveren.

Een API wordt niet ontworpen en gebouwd voor een machine, maar voor een gebruiker: een mens! Om een goede gebruikerservaring te bieden is het belangrijk om te weten voor wie ontworpen en gebouwd wordt. Vanuit de landelijke API strategie worden een aantal aanbevelingen gedaan ten aanzien van de ontwikkeling van APIs.

1.2. Standaardisatie van processen

Door standaardisatie van processen is potentieel veel winst te halen voor gemeenten. Op het moment dat gemeenten op hoofdlijn dezelfde processen hanteren, wordt het standaardiseren van de ondersteunende informatiesystemen eenvoudiger dan het nu is, en wordt samenwerking tussen gemeenten en de onderlinge uitwisseling van gegevens (portabiliteit) eenvoudiger en kan gemeentelijke dienstverlening naar inwoners en bedrijven eenduidiger plaats gaan vinden. Standaardisatie van processen leidt daarnaast tot standaardisatie van de vraag om gegevens vanuit de processen. Dit vereenvoudigt, en versnelt, de ontwikkeling van informatiemodellen en daarop gebaseerde APIs.

1.3. Aansluiting op de GEMMA informatiearchitectuur

Het GEMMA Gegevenslandschap is onderdeel van de GEMMA-architectuur. De GEMMA beschreef tot nu toe de bedrijfsarchitectuur en de informatiearchitectuur van gemeenten als een referentiearchitectuur. Gemeenten dienden deze referentiearchitectuur zelf te vertalen naar een lokale gemeentelijke architectuur. Vanuit het gegevenslandschap wordt op onderdelen nu een dwingendere architectuur beschreven. Met name op de onderdelen authenticatie, autorisatie, logging, gebruik en aanbieden van APIs wordt een inrichting beschreven die verplicht is. Deze inrichting heeft bijvoorbeeld impact op de wijze waarop een gemeente moet omgaan met de authenticatie en autorisatie van interne medewerkers. Ook geeft het gegevenslandschap meer dan vroeger aan marktpartijen concrete eisen ten aanzien van de te hanteren softwarearchitectuur. De GEMMA Referentiearchitectuur geeft een breed overzicht van het 'wat' en het GEMMA Gegevenslandschap gaat diep in op het 'hoe'.

Het GEMMA Gegevenslandschap sluit uiteraard aan bij de GEMMA, maar leidt ook tot aanpassingen in de GEMMA-informatiearchitectuur. Vanuit de visie van het GEMMA Gegevenslandschap moeten informatiesystemen die zich nu als 'silo's' manifesteren worden opgeknipt. Processen worden gescheiden van gegevens en standaard functies als authenticatie, autorisatie en logging worden ondergebracht in aparte componenten. Dit zal leiden tot aanpassingen van de bestaande GEMMA-referentiecomponenten. Een voorbeeld is de *'Inkomenscomponent'*. Deze component bevat nu de inkomensprocessen én opslag van de inkomensgegevens. In de visie van het GEMMA Gegevenslandschap zal deze component worden opgesplitst in een component die de inkomensprocessen afhandelt, en een component die de inkomensgegevens verwerkt. Deze laatste component wordt in het gegevenslandschap niet langer een referentiecomponent genoemd maar een *'register'*. De huidige *Inkomenscomponent* wordt dus opgesplitst naar een *Inkomensregister* en een *Inkomensprocessencomponent*.

Omdat deze ingreep impact zal hebben op de GEMMA Informatiearchitectuur en de daaraan gekoppelde referentiecomponenten in de Softwarecatalogus, worden deze wijzigingen niet direct *rücksichtlos* doorgevoerd. Dat zou op korte termijn enkel leiden tot een vermenigvuldiging van het huidige aantal referentiecomponenten met twee. Enkel indien een register beschikbaar komt dat via een gestandaardiseerd informatiemodel en

een wettelijke grondslag kennen of een toestemming van een burger voor de verwerking van gegevens zijn. Bij gebruik van een dienst wordt de doelbinding vastgelegd zodat de gemeente op een later moment de rechtmatigheid van de verwerking van de gegevens kan aantonen.

Integratiefunctie – de door dienstenaanbieders beschikbaar gestelde diensten worden via een veilige infrastructuur ontsloten naar dienstenafnemers. Deze infrastructuur bestaat uit een combinatie van afspraken, standaarden en voorzieningen. Onderdelen van de integratiefunctie zijn onder andere de fysieke netwerken die gebruikt worden voor uitwisseling van gegevens, beveiligingsdiensten ten aanzien van de gegevensuitwisseling (SIEM/SOC) en voorzieningen voor het kunnen vinden en gebruiken van diensten.

Dienstenaanbieder – een dienstenaanbieder levert via diensten gegevens aan afnemers. Deze diensten leveren gegevens of informatie en worden bij voorkeur geleverd in de vorm van gestandaardiseerde API's van (bijv. RESTful³ of SOAP) webservices. Diensten conformeren zich aan de binnen de overheid gemaakte afspraken ten aanzien van diensten.⁴ Dienstenaanbieders borgen dat alleen geautoriseerde en geauthentiseerde afnemers toegang krijgen tot diensten. Het gebruik van diensten wordt ten behoeve van transparantie- en verantwoordingsdoeleinden in logbestanden bijgehouden.

De gegevens die door een dienstenaanbieder worden geboden kunnen gegevens uit een basisregistratie, een gemeentelijke kernregistratie of sectorale gegevens betreffen⁵.

bijbehorende standaard diensten ontsloten wordt, zullen de bestaande GEMMA-referentiecomponenten aangepast worden.

Een andere wijziging is dat er in het GEMMA Gegevenslandschap zuiverder wordt gekeken naar gegevensopslag dan in het verleden het geval was. Een voorbeeld is de GEMMA Zaakregistratiecomponent. Deze component registreert zaken conform het informatiemodel zaken (RGBZ). In dit informatiemodel worden zaken gemodelleerd, maar bijvoorbeeld ook besluiten en documenten. Voor besluiten en documenten geldt dat deze breder worden gebruikt dan alleen bij zaakgericht werken. Om die reden worden deze objecten uit het informatiemodel verwijderd en als aparte informatiemodellen en registers (besluitenregister en documentenregister) gepositioneerd. Er ontstaan in het GEMMA Gegevenslandschap dus veel registers. Kenmerk van de registers is dat de daarin opgeslagen gegevens meervoudig gebruikt kunnen worden en deze de bron vormen voor de informatieobjecten die er in zijn opgeslagen. In de registers worden geen redundante gegevens bijgehouden.

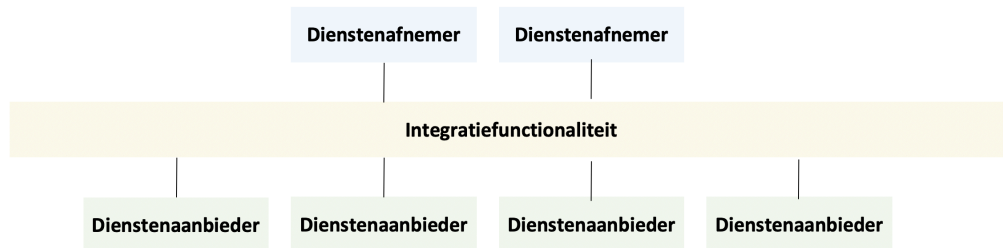
³ https://nl.wikipedia.org/wiki/Application_programming_interface

⁴ Onder andere de landelijke API strategie voor restful APIs (<https://www.geonovum.nl/themas/kennisplatform-apis>)

⁵ Zie ook https://www.gemmaonline.nl/index.php/GMT_Typering_van_gegevens

1.4. Bevraging bij de bron

Belangrijk uitgangspunt van het GEMMA Gegevenslandschap is dat gegevens bij gebruik uit de bron worden opgehaald. Gegevens worden dus niet redundant opgeslagen in eigen registers. Een afnemer haalt op het moment dat gegevens nodig zijn deze op via diensten (APIs) die door de dienstenaanbieder worden geboden.



Figuur 2 - Netwerk van dienstenaanbieders en dienstenaanbieders

In het GEMMA Gegevenslandschap wordt met een bronregister de bron bedoeld waar de gegevens authentiek zijn opgeslagen. Omdat gemeenten bronhouder zijn van de persoonsgegevens van hun inwoners, bestaan er voor deze persoonsgegevens dus net zoveel bronregisters als er gemeenten zijn. Dat betekent niet dat de GBA-V niet als een bron voor persoonsgegevens kan worden gebruikt. Het gebruik van een dergelijke voorziening is een oplossing als het raadplegen van het authentieke bronregister niet mogelijk of niet praktisch is. In het geval van de bronregisters van persoonsgegevens zou het bijvoorbeeld zo moeten zijn dat al deze bronregisters van gemeenten 24x7 bevragebaar moeten zijn voor externe partijen. Dat is in de praktijk niet zo, waardoor het bevragen van de gemeentelijke GBA-registers geen praktische optie is. In dit geval biedt bevraging van een landelijke voorziening een haalbaar alternatief voor bevraging bij bronregisters. In de visie van het GEMMA Gegevenslandschap zijn landelijke voorzieningen tijdelijke voorzieningen. Zodra het technisch en organisatorisch mogelijk is om de bronhouders te bevragen dienen landelijke voorzieningen uitgefaseerd te worden.

Het is uitdrukkelijk de bedoeling om redundante opslag van gegevens te voorkomen en gegevens te bevragen bij de bron. Het is echter mogelijk dat er redenen zijn om binnengemeentelijk toch informatiesystemen te hanteren die geen gebruik maken van dit architectuurpatroon. Dit kan bijvoorbeeld het geval zijn bij systemen die breder worden gebruikt dan enkel de gemeentelijke markt. Denk hierbij bijvoorbeeld aan een financieel- of HR-systeem of document management systeem wat ook in de private sector wordt toegepast. Een dergelijk systeem zal bijvoorbeeld persoonsgegevens redundant opslaan aangezien die systemen bij inzet in de private sector geen toegang krijgen tot de basisregistratie personen. De gemeente heeft in dat geval geen andere keuze dan accepteren dat er gegevens redundant worden opgenomen.

De gemeente dient wel maatregelen te nemen om de kwaliteit en de toegang tot en gebruik van redundante gegevens te borgen. Een andere reden om gegevens redundant op te slaan kan zijn dat een bron niet kan voldoen aan de gewenste SLA, bijvoorbeeld doordat de bron de gewenste responsetijden niet haalt, geen historie bijhoudt of niet 24x7 beschikbaar is. Als een bron wel voldoet aan alle eisen die gesteld worden aan de bron, dan is het wel de bedoeling dat de bron ook direct bevrage wordt en de gegevens niet meer redundant opgeslagen worden.

1.5. Authenticatie en autorisatie

Toegang tot diensten wordt alleen verleent aan personen, organisaties of systemen die op een niveau zijn geauthentiseerd wat past bij de dienst. Het betrouwbaarheidsniveau van een dienst is afhankelijk van de gegevens die door de dienst verwerkt worden en moet per dienst vastgesteld worden⁶. Het authenticatiemiddel wat gebruikt wordt voor de toegang tot een dienst moet hetzelfde of een hoger niveau hebben dan het betrouwbaarheidsniveau van de dienst. Voor gebruik van een dienst die geclassificeerd is op betrouwbaarheidsniveau 'substantieel', is dus minimaal een authenticatiemiddel op niveau 'substantieel' vereist.

Uitgangspunt bij de autorisatie in het GEMMA Gegevenslandschap is dat gemeenten intern zelf de authenticatie en autorisatie van gebruikers regelen. Binnen de autorisaties regelt de gemeente welke medewerker, of rol, bevoegd is voor het gebruiken van welke functie van een informatiesysteem. Hierbij heeft het de voorkeur om hiervoor een systeem te implementeren waarbij de autorisaties centraal worden bijgehouden (via bijvoorbeeld een Identity en Access Management systeem of Identity Management systeem)⁷ zodat grip gehouden kan worden op de verschillende toegekende autorisaties van gebruikers.

Binnen het GEMMA Gegevenslandschap wordt het principe van gedelegeerde autorisatie gehanteerd. Indien een dienst gegevens afneemt van een dienstenaanbieder, is het uitgangspunt dat deze dienstenaanbieder de dienst authenticert op het niveau van de identiteit van de afnemer. Er is dus sprake van de aggregatie van identiteit van een specifiek niveau (bijvoorbeeld een gemeentelijke professional) naar een generiek niveau (de gemeente). Bij een aanroep van een dienst worden als metagegevens onder andere de identiteit van de aanroepende partij en de doelbindingsclaim voor de verwerking doorgegeven. Beide metagegevens worden door de dienstenaanbieder in logging opgenomen zodat verantwoording over het gebruik van de diensten mogelijk is.

Een voorbeeld ter illustratie van het bovenstaande:

Functionaliteit voor het afgeven van een gemeentelijke parkeervergunning raadpleegt de GBA-V. Bij de aanroep van de GBA-V wordt door gemeente de identiteit van de gemeentelijke professional omgezet naar "gemeente xxx". Door de GBA-V wordt vervolgens geautoriseerd op niveau "gemeente xxx mag inwoners muteren en de rest van Nederland raadplegen". Door de gemeente wordt vastgelegd welke gemeentelijke professional de persoonsgegevens heeft geraadpleegd in het kader van het afgeven van een gemeentelijke parkeervergunning en door de GBA-V wordt vastgelegd dat de gemeente xxx een raadpleging van een persoon heeft gedaan in het kader van het afgeven van een gemeentelijke parkeervergunning.

Via de inrichting van gedelegeerde autorisatie en expliciete duiding van de doelbindingsclaim door de afnemer kan auditing achteraf plaatsvinden. Toetsing of elke organisatie rechtmatig heeft gehandeld is hiermee in te richten. Doelbinding wordt vooraf bepaald, terwijl achteraf door middel van audits kan worden bepaald of de door

⁶ <https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus>

⁷ https://en.wikipedia.org/wiki/Identity_management

een organisatie gebruikte doelbindingsclaims rechtmatig waren: *‘vertrouwen vooraf, controle achteraf’*. Dit leidt tot een beheersbare en overzichtelijke inrichting van autorisaties.

1.6. Open en gesloten gegevens

Door gemeenten worden verschillende typen gegevens verwerkt. Enerzijds worden gegevens verwerkt die alleen worden verstrekt aan afnemers die daarvoor geautoriseerd zijn of toestemming hebben gekregen (gesloten gegevens), en anderzijds worden gegevens verwerkt die een openbaar karakter hebben (open gegevens). De overheid biedt een leidraad⁸ ten aanzien van welke gegevens classificeren als open gegevens.

Voor wat betreft open gegevens worden geen eisen gesteld aan de autorisatie en authenticatie van afnemers. Open gegevens zijn toegankelijk zonder dat er enige vorm van registratie van gegevens van de potentiële gebruiker plaatsvindt. Voor gesloten gegevens ligt dit anders.

Die eisen die gesteld worden aan de verwerking van gegevens zijn onder andere afhankelijk van de typering van de gegevens die door een dienst worden verwerkt. Er kan een verschil zijn in de manier waarin met open en gesloten gegevens wordt omgegaan. Voor diensten die open gegevens verwerken kunnen bijvoorbeeld op het gebied van authenticatie, autorisatie en transport van de gegevens andere eisen worden gesteld dan aan diensten die gevoelige gegevens verwerken. Open gegevens kunnen bijvoorbeeld via een internetverbinding worden uitgewisseld terwijl voor gesloten gegevens geldt dat veelal hiervoor een gesloten netwerk zoals GGI-Netwerk wordt gebruikt.

Het is echter niet zo dat het type gegeven van een dienst 1:1 te vertalen is naar maatregelen die genomen moeten worden. Het is bijvoorbeeld mogelijk dat een gemeente er voor kiest om open gegevens toch via een private verbinding zoals GGI-Netwerk en tweezijdig TLS in te richten. Reden hiervoor kan zijn dat de gemeente een zo hoog mogelijke mate van zekerheid wil hebben dat de gegevens in het transport niet gemanipuleerd kunnen worden. Gemeenten dienen dus per dienst te bepalen welke maatregelen genomen moeten worden. De AVG en BIO bieden hiervoor richtlijnen maar gemeenten zijn er zelf verantwoordelijk voor hierin een afweging te maken.

1.7. Doelbinding voor gegevensverwerking

Voor de verwerking van persoonsgegevens is conform privacywetgeving een doel en een verwerkingsgrondslag vereist. De grondslag kan bijvoorbeeld bestaan uit een wettelijke verplichting, of toestemming die een persoon heeft afgegeven ten aanzien van de verwerking van zijn of haar gegevens. Het doel geeft aan waarvoor de gegevens verwerkt worden. In dit document noemen we de combinatie van doel en grondslag de *doelbinding*. Uitgangspunt binnen het GEMMA Gegevenslandschap is dat afnemers bij ieder verzoek om gegevens, ongeacht of dit persoonsgegevens zijn, de doelbindingsclaim aangeven voor de verwerking. Indien vanuit een eindgebruikersfunctie gegevens worden ‘verwerkt’⁹ dan wordt door deze functie de doelbindingsclaim voor de

⁸ <https://data.overheid.nl/ondersteuning/open-data/wat-is-open-data>

⁹ EU-AVG artikel 4: "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde

verwerking vastgelegd. Deze doelbindingsclaim is een verklaring van de afnemer over doel en grondslag van de verwerking. Deze claim wordt bij elke verwerking ten behoeve van transparantie en verantwoordingsdoeleinden in logbestanden vastgelegd. In deze logbestanden worden onder andere de gebruikte dienst, de eindgebruiker en de doelbindingsclaim vastgelegd. De logbestanden kunnen achteraf worden gebruikt om een audittrail samen te stellen die gebruikt kan worden voor het achteraf bepalen of de verwerking van gegevens rechtmatig is geweest.

Doelbindingsclaims voor gemeenten worden, zover dat mogelijk is, door gemeenten onder regie van VNG Realisatie gestandaardiseerd. Dit betreft de verwerkingsgronden voor privaats- als publiekrechtelijke taken met een wettelijke grondslag of voortkomend uit een lokale verordening en de doelbindingen die op basis van een toestemming van een burger verleend kunnen worden. Door deze standaardisatie wordt gewaarborgd dat de verwerkingsgronden tussen gemeenten onderling vergelijkbaar, en juridisch gevalideerd zijn.

Verwerkingen die door een dienstenafnemer of dienstenaanbieder worden uitgevoerd worden vastgelegd in logbestanden. Bij de logging van de verwerking wordt opgenomen wat de doelbindingsclaim voor de verwerking is zodat zowel naar de burger als bestuur transparant verantwoording kan worden afgelegd over gegevensverwerkingen. Zowel bij de dienstenafnemer als bij de dienstenaanbieder wordt een logbestand aangelegd. De partij die de verwerking initieert stelt een uniek logtransactie-id samen wat door alle partijen binnen de transactie wordt gebruikt bij de vastlegging van logregels. Via dit logtransactie-id zijn logbestanden van dienstenaanbieders en -afnemers aan elkaar te relateren waardoor een audittrail kan worden samengesteld.

1.8. Privacy en security

Een van de uitgangspunten van het GEMMA Gegevenslandschap is zorg dragen voor een goede beveiliging van gegevens en garanderen van de bescherming van de privacy. Om invulling te kunnen geven aan zowel verwachtingen van de burger als de wettelijke vereisten realiseren wordt een samenhangend geheel van technische, organisatorische, fysieke en procedurele maatregelen beschreven.

Het Blauwe Boekje van Jaap-Henk Hoepman¹⁰ geeft generieke ontwerpstrategieën die gevolgd kunnen worden voor het borgen van de privacy. Vanuit het GEMMA Gegevenslandschap worden deze ontwerpstrategieën omarmt. De ontwerpstrategieën zijn onderverdeeld in twee groepen: data georiënteerde strategieën en proces georiënteerde strategieën.

De data georiënteerde strategieën van het Blauwe Boekje zijn gericht op de privacy vriendelijke verwerking van de data zelf en zijn dus technisch van aard.

- Minimaliseer (Minimise)
Beperk zo veel mogelijk de verwerking van persoonsgegevens.
- Scheid (Separate)

procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

¹⁰ <https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf>

- Scheid de verwerking van persoonsgegevens zo veel mogelijk van elkaar.
- Abstraheer (Abstract)
Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.
- Verberg (Hide)
Bescherm persoonsgegevens, of maak ze onherleidbaar of onobserveerbaar. Voorkom dat persoonsgegevens openbaar worden.

De proces georiënteerde strategieën zijn gericht op de processen rond de verwerking van persoonsgegevens. Ze gaan over de organisatorische aspecten en de noodzakelijke procedures.

- Informeer (Inform)
Informeert gebruikers over de verwerking van hun persoonsgegevens.
- Geef controle (Control)
Geef gebruikers controle over de verwerking van hun persoonsgegevens.
- Dwing af (Enforce)
Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing deze af.
- Toon aan (Demonstrate)
Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.

Op de verschillende ontwerpstrategieën zijn binnen het GEMMA Gegevenslandschap uitgangspunten en functies gedefinieerd die bijdragen aan de implementatie van de ontwerpstrategie. Voorbeelden hiervan zijn:

- Eenmalige registratie en bevraging bij de bron. Hierdoor wordt de kans op datalekken en onbevoegde verwerkingen van gegevens verkleind doordat gegevens nog maar op één plek worden bijgehouden;
- Diensten worden 'smal' gehouden en zijn toegespitst op de levering van gegevens voor een specifiek doel. Hierdoor is gegevens en informatieverstrekking naar afnemers proportioneel;
- Toegang tot diensten wordt verleend onder voorwaarde van een doelbinding van de afnemer;
- Logging van alle activiteiten waar men vanuit wetgeving toe verplicht is, of waaraan vanuit de business of beveiliging behoefte aan is. Dit maakt auditing op de rechtmatigheid van de verwerking van gegevens en diensten mogelijk;
- Afstemming van het beveiligingsniveau van de diensten op het authenticatiemiddel van de afnemer van de dienst.

Naast deze uitgangspunten vanuit de architectuur worden bij implementatie van een voorziening uiteraard ook specifieke maatregelen genomen. Deze maatregelen zijn op hoofdlijnen beschreven in de Baseline Informatiebeveiliging Overheid (BIO).¹¹

1.9. Standaardisatie via informatiemodellen

Gemeenten nemen, met ondersteuning van VNG Realisatie, de regie over de standaardisatie van de gemeentelijke gegevens. Daar waar anno 2018 slechts een klein deel van de gemeentelijke gegevens via

¹¹ <https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/>

informatiemodellen is gestandaardiseerd (RSGB, RGBZ, ImZTC, ImGeo en Raadsinformatie), worden in de nieuwe inrichting op termijn ook gemeentelijke kernregistraties en sectorale registraties gestandaardiseerd via informatiemodellen. Dit betekent dat nieuwe informatiemodellen ontwikkeld worden voor bijvoorbeeld het sociaal- en het belastingen domein en dat aansluiting gezocht wordt bij bestaande informatiemodellen zoals het IMBOR¹² voor de openbare ruimte. Het is mogelijk dat binnen omvangrijke domeinen een opsplitsing naar sub-domeinen of thema's wordt gemaakt en daardoor binnen een domein meerdere informatiemodellen ontstaan. Denk hierbij bijvoorbeeld aan het sociaal domein. Dit domein omvat een groot aantal taken, waardoor opsplitsing in kleinere delen voor de hand ligt. Te denken valt dan bijvoorbeeld aan aparte informatiemodellen voor de taken die gemeenten hebben ten aanzien van de jeugdzorg, maatschappelijke ondersteuning en werk en inkomen.

Door het standaardiseren van informatiemodellen is standaardisatie van de toegang tot gegevens via diensten mogelijk. Op het moment dat vanuit dienstverlening een door gemeenten breed gedeelde behoefte aan gegevens ontstaat, kan er een standaardisatietraject starten. In dit traject wordt samen met gemeenten en marktpartijen de behoefte aan gegevens voor de betreffende processen geïnventariseerd, waarna vanuit deze behoefte een informatiemodel wordt ontwikkeld. VNG Realisatie kan regie voeren over de totstandkoming en de inhoud van de modellen. Onderdeel van het regie voeren over informatiemodellen is ook het governance model wat gehanteerd wordt. Per informatiemodel moet worden bepaald wat de meest voor de hand liggende standaardisatiepartij en bijbehorende governancestructuur is.

1.10. Standaardisatie van gegevensontsluiting

Dienstenaanbieders maken gegevens beschikbaar via diensten. Diensten doen dit bij voorkeur via een applicatie interface, ofwel Application Programming Interface (API). Een applicatie-interface is een toegangspunt waar applicatieservices beschikbaar worden gesteld. Binnen de overheid zijn afspraken¹³ gemaakt ten aanzien van de technische- en gebruiksaspecten van APIs. Deze afspraken beogen te bereiken dat binnen de overheid APIs op vergelijkbare wijze werken en beveiligd worden.

De ontwikkeling van APIs wordt afgestemd op vragen die vanuit de dienstverlening en processen worden gesteld. Hierdoor wordt geborgd dat APIs aansluiten op de behoefte die vanuit afnemers leeft. De gegevens die door de APIs worden ontsloten conformeren zich aan de gestandaardiseerde informatiemodellen. Hierdoor wordt de uitwisselbaarheid van gegevens bevorderd, en is voor alle partijen duidelijk wat de syntax, samenhang en betekenis (semantiek) van de gegevens is. Bij de ontwikkeling van diensten worden marktpartijen in een vroeg stadium betrokken, aangezien zij uiteindelijk de partijen zijn die de diensten realiseren en leveren.

Een API wordt niet ontworpen en gebouwd voor een machine, maar voor een gebruiker: een mens! Om een goede gebruikerservaring te bieden is het belangrijk om te weten voor wie ontworpen en gebouwd wordt. Vanuit

¹² <https://www.geonovum.nl/geo-standaarden/overzicht-informatiemodellen-nen3610-familie/informatiemodel-beheer-openbare-ruimte>

¹³ <https://docs.geostandaarden.nl/api/API-Strategie/>

de landelijke API strategie worden een aantal aanbevelingen¹⁴ gedaan ten aanzien van de ontwikkeling van APIs.

1.11. Standaardisatie van processen

Door standaardisatie van processen is potentieel veel winst te halen voor gemeenten. Op het moment dat gemeenten op hoofdlijn dezelfde processen hanteren, wordt het standaardiseren van de ondersteunende informatiesystemen eenvoudiger dan het nu is, en wordt samenwerking tussen gemeenten en de onderlinge uitwisseling van gegevens (portabiliteit) eenvoudiger en kan gemeentelijke dienstverlening naar inwoners en bedrijven eenduidiger plaats gaan vinden. Standaardisatie van processen leidt daarnaast tot standaardisatie van de vraag om gegevens vanuit de processen. Dit vereenvoudigt, en versnelt, de ontwikkeling van informatiemodellen en daarop gebaseerde APIs.

1.12. Aansluiting op de GEMMA informatiearchitectuur

Het GEMMA Gegevenslandschap is onderdeel van de GEMMA-architectuur. De GEMMA beschreef tot nu toe de bedrijfsarchitectuur en de informatiearchitectuur van gemeenten als een referentiearchitectuur. Gemeenten dienden deze referentiearchitectuur zelf te vertalen naar een lokale gemeentelijke architectuur. Vanuit het gegevenslandschap wordt op onderdelen nu een dwingendere architectuur beschreven. Met name op de onderdelen authenticatie, autorisatie, logging, gebruik en aanbieden van APIs wordt een inrichting beschreven die verplicht is. Deze inrichting heeft bijvoorbeeld impact op de wijze waarop een gemeente moet omgaan met de authenticatie en autorisatie van interne medewerkers. Ook geeft het gegevenslandschap meer dan vroeger aan marktpartijen concrete eisen ten aanzien van de te hanteren softwarearchitectuur. De GEMMA Referentiearchitectuur geeft een breed overzicht van het 'wat' en het GEMMA Gegevenslandschap gaat diep in op het 'hoe'.

Het GEMMA Gegevenslandschap sluit uiteraard aan bij de GEMMA, maar leidt ook tot aanpassingen in de GEMMA-informatiearchitectuur. Vanuit de visie van het GEMMA Gegevenslandschap moeten informatiesystemen die zich nu als 'silo's' manifesteren worden opgeknipt. Processen worden gescheiden van gegevens en standaard functies als authenticatie, autorisatie en logging worden ondergebracht in aparte componenten. Dit zal leiden tot aanpassingen van de bestaande GEMMA-referentiecomponenten. Een voorbeeld is de *'Inkomenscomponent'*. Deze component bevat nu de inkomensprocessen én opslag van de inkomensgegevens. In de visie van het GEMMA Gegevenslandschap zal deze component worden opgesplitst in een component die de inkomensprocessen afhandelt, en een component die de inkomensgegevens verwerkt. Deze laatste component wordt in het gegevenslandschap niet langer een referentiecomponent genoemd maar een *'register'*. De huidige *Inkomenscomponent* wordt dus opgesplitst naar een *Inkomensregister* en een *Inkomensprocessencomponent*.

Omdat deze ingreep impact zal hebben op de GEMMA Informatiearchitectuur en de daaraan gekoppelde referentiecomponenten in de Softwarecatalogus, worden deze wijzigingen niet direct *rücksichtlos* doorgevoerd.

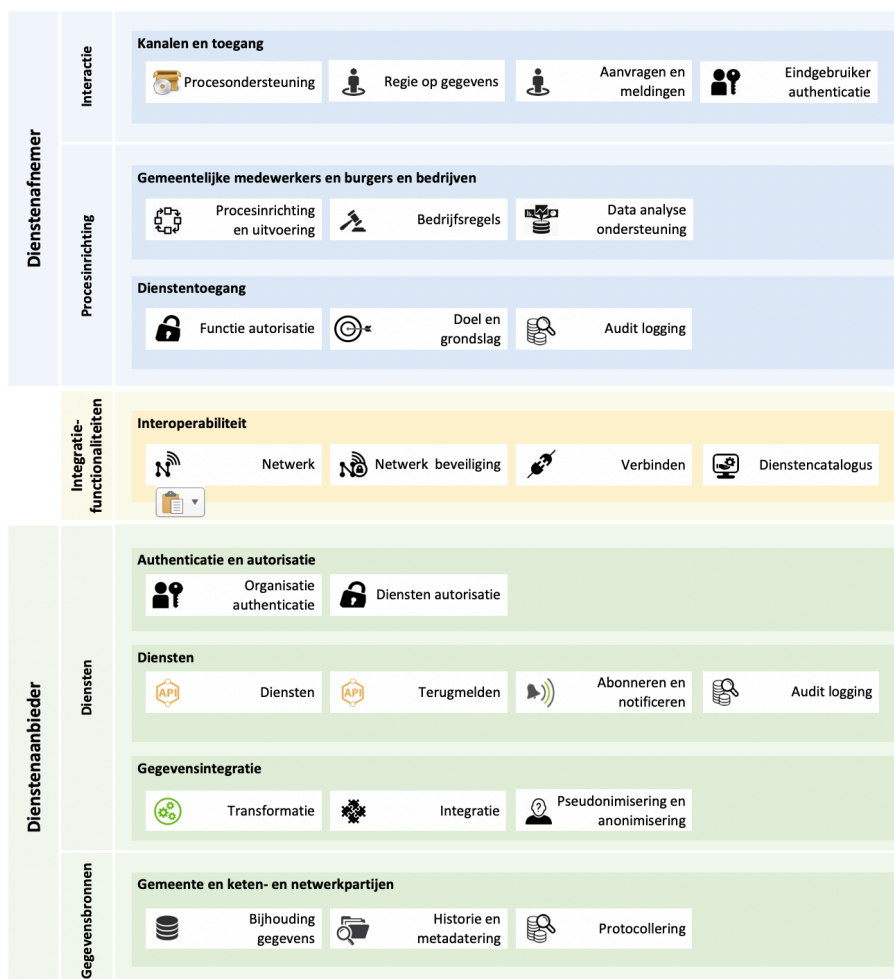
¹⁴ <https://docs.geostandaarden.nl/api/cv-hr-API-Strategie-20190213/#specifieke-aanbevelingen-voor-een-goede-dx>

Dat zou op korte termijn enkel leiden tot een vermenigvuldiging van het huidige aantal referentiecomponenten met twee. Enkel indien een register beschikbaar komt dat via een gestandaardiseerd informatiemodel en bijbehorende standaard diensten ontsloten wordt, zullen de bestaande GEMMA-referentiecomponenten aangepast worden.

Een andere wijziging is dat er in het GEMMA Gegevenslandschap zuiverder wordt gekeken naar gegevensopslag dan in het verleden het geval was. Een voorbeeld is de GEMMA Zaakregistratiecomponent. Deze component registreert zaken conform het informatiemodel zaken (RGBZ). In dit informatiemodel worden zaken gemodelleerd, maar bijvoorbeeld ook besluiten en documenten. Voor besluiten en documenten geldt dat deze breder worden gebruikt dan alleen bij zaakgericht werken. Om die reden worden deze objecten uit het informatiemodel verwijderd en als aparte informati modellen en registers (besluitenregister en documentenregister) gepositioneerd. Er ontstaan in het GEMMA Gegevenslandschap dus veel registers. Kenmerk van de registers is dat de daarin opgeslagen gegevens meervoudig gebruikt kunnen worden en deze de bron vormen voor de informatieobjecten die er in zijn opgeslagen. In de registers worden geen redundante gegevens bijgehouden.

2. Uitwerking GEMMA Gegevenslandschap

Onderstaand figuur toont het uitgewerkte model van het GEMMA Gegevenslandschap. In dit model gebruiken gemeenten, keten- en netwerkpartijen en burgers en bedrijven (eindgebruikers) gebruikersinterfaces die geboden worden vanuit proces- en analysesystemen en mobiele applicaties. De gegevens die door deze systemen worden verwerkt, worden via een veilige landelijke infrastructuur via gestandaardiseerde diensten afgenomen van dienstenaanbieders.



Figuur 3 – Functies van het GEMMA Gegevenslandschap

De GEMMA Gegevenslandschap visualisatie is bedoeld om discussies te kunnen voeren over de globale architectuur, het is geen plaat met formele architectuurbouwstenen zoals in de GEMMA-referentiearchitectuur. De functies in bovenstaande figuur zijn dan ook niet 1:1 te vertalen naar concrete Archimate-elementen. Ze geven een bepaald type functionaliteit weer waar op verschillende manier invulling aan kan worden gegeven. In sommige gevallen is een functie te vertalen naar applicaties of functies daarvan maar in andere gevallen, zoals bij het blokje "Eindgebruiker authenticatie" en "Functie autorisatie", is er sprake van een complex samenspel van processen en voorzieningen. Iedere functie van het GEMMA Gegevenslandschap is, of wordt, nader uitgewerkt in een formeel architectuurdocument.

2.1. Interactie

De interactielaag van het GEMMA Gegevenslandschap bevat functionaliteit die nodig is voor het leveren van gebruikersinterfaces aan afnemers van diensten. De eindgebruiker kan een medewerker van de gemeente zijn, maar ook een inwoner of ondernemer.



2.1.1. Procesondersteuning

Ondersteuning voor gemeentelijke processen zoals het heffen van belastingen, het uitkeren van uitkeringen, het ondersteunen van burgers die maatschappelijke ondersteuning nodig hebben en het onderhouden van de openbare ruimte wordt geboden door informatiesystemen. Procesondersteunende informatiesystemen worden primair gebruikt door medewerkers van de gemeente. Het is echter ook mogelijk dat bedrijven systemen voor procesondersteuning gebruiken in combinatie met gegevens van de overheid. Denk hierbij bijvoorbeeld aan een architectenbureau dat ontwerpsoftware (CAD-systeem) gebruikt en daarbij gegevensbronnen van de overheid ontsluit.

De gebruikersschermen van processystemen kunnen schermen zijn die 1:1 gekoppeld zijn aan de procesinrichting en uitvoering van de proceslaag. In dat geval worden de interactie en de procesinrichting vanuit één informatiesysteem geleverd en kan de eindgebruiker beperkt invloed uitoefenen op de manier en waarop schermen worden weergegeven. Het is ook mogelijk dat vanuit de procesinrichting en uitvoering schermen dynamisch worden gegenereerd op basis van een geconfigureerde procesinrichting en bedrijfsregels. Hierbij kan bijvoorbeeld van uitvoerbare BPMN of vergelijkbare technieken gebruik gemaakt worden.

2.1.2. Regie op gegevens

Voor burgers worden een aantal generieke diensten ontsloten op het gebied van regie op hun eigen gegevens. Onder deze diensten vallen onder andere het recht op inzage en correctie van eigen gegevens, en het recht om de verwerkingen van hun gegevens door gemeenten en ketenpartijen in te zien. Als alle overheden en bestuursorganen deze functies op een eigen manier invullen dan zien burgers door de bomen het bos niet meer. Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is daarom besloten om te komen tot afspraken over hoe we de dienstverlening aan burgers en ondernemers voor verschillende generieke functies willen inrichten. Deze afspraken worden vastgelegd in beleidskaders als uitwerking van het 'Beleidskader digitale basisinfrastructuur'. Door BZK wordt gewerkt aan een beleidsnotitie digitale portalen (zoals MijnOverheid).

Vanuit het GEMMA Gegevenslandschap worden de generieke diensten op het gebied van regie op hun eigen gegevens gefaciliteerd via de functie 'Regie op gegevens'. Deze functie biedt de volgende functionaliteit:

- *Inzage geven in de 'eigen' gegevens van de burger* – via deze functie kan de burger inzien welke gegevens een gemeente van de burger bijhoudt;
- *Inzage in het gebruik van gegevens* – via deze functie kan de burger zien welke gegevens door de gemeente zijn gebruikt binnen gemeentelijke processen of zijn uitgewisseld met keten- en netwerkpartijen en voor welk doel dit was;
- *Correctie van incorrecte gegevens* – deze functie biedt aan burgers en bedrijven de mogelijkheid om de gemeente te verzoeken gegevens die naar mening van de burger incorrect zijn te corrigeren. Deze functionaliteit is vergelijkbaar met de functionaliteit voor terugmelden van de basisregistraties;
- *Toestemming voor uitwisseling gegevens* – burgers hebben de mogelijkheid om, daar waar uitwisselingen bovenwettelijk zijn, per gegevensuitwisseling aan te geven met welke partijen de gemeente deze partijen gegevens mag delen;

Bovenstaande functies dragen bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen. Functionaliteit hiervoor kan bijvoorbeeld worden geboden via een landelijke of gemeentelijke PIP en/of via een andersoortige voorziening zoals een app.

2.1.3. Aanvragen en meldingen

Inwoners en ondernemers hebben de mogelijkheid om meldingen te doen en producten en diensten aan te vragen bij de gemeente. Denk hierbij bijvoorbeeld aan het melden van een niet werkende lantaarnpaal via een melding openbare ruimte (MOR) of het aanvragen van een uittreksel uit de gemeentelijke basisregistratie personen. Door gebruikers wordt voor het gebruik van deze diensten over het algemeen gebruik gemaakt van formulieren in het digitaal loket van de gemeente of een app op een telefoon of tablet. Inwoners en ondernemers kunnen ook online berichten met de gemeente uitwisselen. Bijvoorbeeld over lopende zaken of naar aanleiding van ontvangen formele berichten via de landelijke Berichtenbox.

2.1.4. Eindgebruiker authenticatie

Het is de verantwoordelijkheid van de gemeente om daar waar nodig gebruikers te authenticeren voordat diensten ter beschikking worden gesteld. De dienstenafnemer moet hierbij waarborgen dat het gebruikte authenticatiemiddel past bij het betrouwbaarheidsniveau van de dienst die de eindgebruiker gaat gebruiken. Indien bijvoorbeeld binnen een functie jeugdzorg gegevens worden verwerkt, dan zal daarvoor een hoger authenticatieniveau vereist zijn dan wanneer alleen 'gewone' persoonsgegevens verwerkt worden. In het eerste geval zal naar verwachting gezien de gevoeligheid van de gegevens een middel op niveau 'hoog' vereist zijn, terwijl bij gewone persoonsgegevens volstaan kan worden met een middel op niveau 'laag' of 'substantieel'. Door het Forum Standaardisatie is een handreiking¹⁵ opgesteld die gemeenten kunnen gebruiken voor het bepalen van het betrouwbaarheidsniveau van diensten. Gemeenten moeten per dienst ook bepalen of het nodig

¹⁵ <https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus>

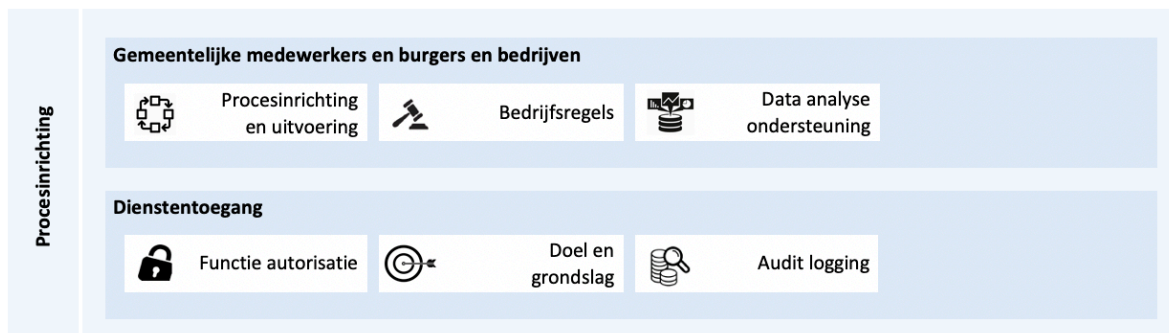
is om een burger zich te laten authenticeren. Voor bijvoorbeeld een melding openbare ruimte of het maken van een afspraak bij de gemeente is het bijvoorbeeld niet noodzakelijk om een authenticatiemiddel toe te passen. Bij deze diensten voldoet het om de burger zelf de identificerende gegevens in te laten voeren of de melding anoniem te laten opvoeren.

De beschikbare authenticatiemiddelen voor burgers worden vastgesteld in het landelijke eID-programma¹⁶. Het gaat hierbij om door de overheid verschaft authenticatiemiddelen op verschillende betrouwbaarheidsniveaus (laag, substantieel en hoog) en één of meer door marktpartijen aangeboden (private) middelen op niveaus substantieel en hoog. Voor gebruik binnen het BSN-domein verschaft de overheid de DigiD-middelen. Naast de DigiD-middelen wordt door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ook gewerkt aan een raamwerk voor toelating van private middelen voor het BSN-domein¹⁷. Voor bedrijven en medewerkers van bedrijven kan voor authenticatie gebruik worden gemaakt van een zogenaamd eHerkenningmiddel¹⁸. De eHerkenningmiddelen zijn op verschillende betrouwbaarheidsniveaus beschikbaar.

Naast de landelijke authenticatiemiddelen die de gemeente voor de authenticatie van burgers en bedrijven kan gebruiken, moet de gemeente ook voor de gemeentelijke medewerkers een authenticatiesysteem inrichten.

2.2. Procesinrichting

De procesinrichtinglaag van het GEMMA Gegevenslandschap bevat de functies die van belang zijn voor het inrichten en uitvoeren van processen en bijbehorende bedrijfsregels, het ondersteunen van data analyse en beschrijvende en verklarende statistiek, en het op een compliant aan vigerende wet- en regelgeving wijze gebruiken van gegevensverwerkende diensten. Deze functies zijn nodig om de functies/diensten uit de interactielaag te kunnen bieden..



¹⁶ <https://www.digitaleoverheid.nl/dossiers/eid/>

¹⁷ Situatie september 2019

¹⁸ <https://www.digitaleoverheid.nl/dossiers/eherkenning/>

2.2.1. Procesinrichting en uitvoering

De procesinrichting bevat de functionaliteit die bedoeld is voor het configureren en uitvoeren van processen. Deze functionaliteit komt overeen met wat vroeger ook wel 'workflow'-functionaliteit werd genoemd en tegenwoordig wordt geleverd door BPM-systemen. Hierbij horen vragen als "in welke volgorde kunnen de schermen worden doorlopen?" En "welke diensten moeten worden aangeroepen voor welke berekening?". Deze functionaliteit is nodig om in de interactielaag de juiste schermen met daarop de juiste gegevens te kunnen tonen. Vaak is deze functionaliteit met de schermen verweven in de programmacode van procesapplicaties. Het is (technisch) ook mogelijk om deze processen en gebruikersinterfaces van elkaar te scheiden.

2.2.2. Bedrijfsregels

Gemeenten hebben te maken met regels die gelden bij het uitvoeren van processen. Die zijn voor een deel gebaseerd op wet- en regelgeving waaraan ze moeten voldoen. Aanvullend zijn er regels die beschrijven hoe de gemeente bepaalde processen uitvoert, en op welke manier beslissingen genomen moeten worden. Een voorbeeld van een dergelijke bedrijfsregel is het op basis van zaaktype eigenschappen nagaan of alle benodigde documenten bij een zaakstatus aanwezig zijn. Er zijn geen vastgestelde regels ten aanzien van welke bedrijfsregels in de procesinrichting gehanteerd mogen worden. Daar waar aan gegevens, of de verstrekking van gegevens eisen worden gesteld vanuit wet- of regelgeving is het logisch om deze eisen (bedrijfsregels) binnen de diensten op te nemen die de gegevens leveren. Op die manier wordt gewaarborgd dat deze regels altijd worden uitgevoerd als gegevens uit een bron worden opgehaald of weggeschreven.

Bedrijfsregels kunnen worden 'vastgeklonken' aan de software die zorgt voor de uitvoering van processen, maar ook los van de procesinrichting en uitvoering worden vastgelegd. Dit biedt vooral voordelen in het geval van kennis- en regel-intensieve processen die relatief vaak veranderen. Indien een bedrijfsregel wordt opgenomen binnen een proces, dan wordt deze in de regel uitgeschreven in programmacode door de leverancier van de software, en is die dus niet aanpasbaar door de gemeente. Indien bedrijfsregels los van de procesinrichting en uitvoering worden vastgelegd, dan kan de gemeente de bedrijfsregel desgewenst aanpassen. Dit stelt gemeenten in staat lokaal beleid te implementeren door bedrijfsregels zelf vorm te geven en om bedrijfsregels opnieuw te gebruiken in bijvoorbeeld nieuwe interactievoorzieningen.

Voor het vastleggen van bedrijfsregels los van de procesinrichting en uitvoering wordt veelal gebruik gemaakt van een Business Rule Management Systeem (BRMS¹⁹). Een dergelijk systeem ondersteunt het vastleggen van bedrijfsregels, het muteren en classificeren van die regels, en het controleren van onderlinge consistentie tussen verschillende regels.

2.2.3. Data analyse ondersteuning

Onder data-analyse wordt verstaan de ondersteuning van de analyse van gemeentelijke gegevens en, of in combinatie met, gegevens van keten- en netwerkpartijen, via onder andere beschrijvende en verklarende statistiek. Ondersteuning hiervoor wordt geboden door gespecialiseerde informatiesystemen, waaronder data-warehouse- en analysesystemen. Deze systemen maken gebruik van grote hoeveelheden, vaak samengestelde, gegevens. Het GEMMA Gegevenslandschap faciliteert deze systemen via specifieke gegevensdiensten die gegevens leveren aan de afnemer. Het streven is om real-time analyses op gegevens uit te kunnen voeren, maar waar dit wegens technologische of technische beperkingen nog niet mogelijk is wordt

¹⁹ https://en.wikipedia.org/wiki/Business_rule_management_system

een (asynchrone) levering van gegevens aan afnemers gefaciliteerd. Dit houdt in dat een vraag om een set van gegevens wordt uitgevoerd op een moment dat dit opportuun is. Voor gegevensvragen die grote sets van gegevens opleveren kan dit betekenen dat de vraag, in verband met belasting van de infrastructuur, na kantoor tijd wordt uitgevoerd. Terugkoppeling van de resultaten vindt plaats op een wijze die in overeenstemming is met de gevoeligheid van de gegevens. Voor gegevenssets die geen privacygevoelige gegevens bevatten kan dit bijvoorbeeld via een open data portaal of (s)ftp-verbinding, terwijl voor andere gegevens een beveiligd portaal of 'zandbak'-omgeving nodig is.

Data-analysesystemen worden gebruikt door medewerkers van de gemeente, maar kunnen ook door inwoners en ondernemers worden gebruikt. De data die binnengemeentelijk worden gebruikt voor data-analyse kunnen veelal gesloten data zijn die vanuit privacy-oogpunt niet met derden mag worden gedeeld. De overheidsdata die door ondernemers en burgers gebruikt worden voor data-analyse zijn de open data²⁰, die door de verschillende overheden ter beschikking worden gesteld. Diensten die gegevens bieden voor analysedoeleinden moeten in staat zijn om op aanvraag van de afnemer de gegevens desgewenst te anonimiseren of te pseudonimiseren.

2.2.4. Functie autorisatie

Voor iedere gebruiker die een functie of dienst wil gebruiken, geldt dat bepaald moet worden of de gebruiker daarvoor de benodigde rechten heeft. Deze bepaling start met het bepalen van wie de gebruiker is (identificatie) en de verificatie daarvan (authenticatie). Dit wordt gedaan door de gebruiker via een authenticatiemiddel aan te laten tonen wie hij zegt dat hij is. Dit authenticatiemiddel (bijvoorbeeld DigiD, eHerkenning of lokaal een Identity en Access Management-tool) moet minimaal hetzelfde betrouwbaarheidsniveau hebben als de dienst die gebruikt gaat worden. Nadat met genoeg zekerheid is vastgesteld wie de gebruiker is, is de volgende stap het bepalen of de gebruiker de vereiste rechten heeft voor de functie of dienst die hij of zij wil gebruiken (autorisatie).

Het beheren van autorisaties voor gebruikers vindt bij voorkeur op een centrale plek in de organisatie plaats. Het centraal inrichten van toegangscontrole op functieniveau geeft de meeste waarborgen voor het up-to-date houden van autorisaties. Voor het beheer van identiteiten en autorisaties kan gebruik worden gemaakt van een IAM-tool.

2.2.5. Doel en grondslag

Functies die door eindgebruikers worden gebruikt zullen op een gegeven moment gegevens verwerken. Denk bijvoorbeeld aan een functie die persoonsgegevens bijwerkt in de basisregistratie personen, of een functie die ten behoeve van de gemeentelijke belastingen de gegevens van een kadastraal perceel ophaalt.

Voor iedere verwerking van persoonsgegevens geldt het AVG-uitgangspunt dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. 'Welbepaald en uitdrukkelijk omschreven' houdt in dat geen gegevens verzameld mogen worden zonder dat (vooraf) een precieze doelomschrijving is bepaald. 'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. 'Uitdrukkelijk omschreven' houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben

²⁰ https://nl.wikipedia.org/wiki/Open_data

omschreven. Ten slotte moet er sprake zijn van een wettelijke grondslag voor de verwerking. Voorbeelden van een dergelijke grondslag zijn de toestemming van een betrokkene of een wettelijke verplichting.

Bij het gebruik van een functie moet aangegeven worden voor welk doel en met welke grondslag de functie wordt gebruikt. De combinatie van doel en grondslag wordt in dit document aangeduid als de '*doelbindingsclaim*'. Met deze doelbindingsclaim wordt aangegeven wat het verwerkingsdoel bij het gebruik van de functie is. Het is de verantwoordelijkheid van de gemeente om bij het gebruik van een functie door een gebruiker de juiste doelbindingsclaim te hanteren. Gemeenten moeten daarnaast interne processen ingericht hebben waarmee gewaarborgd wordt dat alleen bevoegden gebruik kunnen maken van functies.

Het is de verplichting van een dienstafnemer (lees: de gemeente) een register van verwerkingsactiviteiten²¹ bij te houden en bij gebruik van applicatiefuncties aan te geven welke verwerkingsgrond bij de uitvoering van de functie van toepassing is. Streven is om de inhoud van dit register landelijk te standaardiseren. Voor een aantal doelbindingsclaims uit het verwerkingenregister zal gelden dat de grondslag van de verwerking wordt gevormd door de expliciete toestemming van de burger. Indien een dienstafnemer van een dergelijke doelbindingsclaim gebruik maakt dan moet deze onomstotelijk kunnen aantonen dat deze expliciete toestemming van de burger voor de verwerking van de gegevens ten tijde van de verwerking verleend was. De burger kan toestemmingen beheren, en dus ook verwijderen, via de regie op gegevens functionaliteit.

2.2.6. Audit logging

Essentieel onderdeel van GEMMA Gegevenslandschap is het bijhouden van het gebruik van gegevens in logbestanden. Uitgangspunt is dat de verwerking van gegevens in logbestanden wordt vastgelegd²², op het moment dat deze gegevens worden verwerkt. Logbestanden kunnen door de gemeente achteraf gebruikt worden om burgers en bedrijven inzage te geven in het gebruik van hun gegevens. Daarnaast dienen de logbestanden als bron voor bijvoorbeeld een externe auditor bij het bepalen of de gemeente gegevens rechtmatig verwerkt heeft. Daartoe wordt in de logbestanden een aantal metagegevens van een verwerking vastgelegd, waaronder de datum en tijd, de gebruiker die de dienst of functie gebruikt, de gehanteerde doelbindingsclaim en de (categorieën van) gegevens die verwerkt zijn.

De plicht om verwerkingen te loggen geldt voor alle organisaties die gegevens verwerken. Het geldt dus voor zowel dienstafnemers als -aanbieders. De integriteit van logbestanden is gezien de rol die zij spelen bij het aantonen van rechtmatig handelen van de gemeente van cruciaal belang. De integriteit van de bestanden moet dus bewaakt worden. Onderdeel van het bewaken van de integriteit van logs is het tegengaan van mutaties in logbestanden en het duurzaam toegankelijk houden van de gegevens.²³

²¹ https://www.gemmaonline.nl/images/gemmaonline/e/e5/Gemeentelijk_gegevenslandschap_-_Register_van_verwerkingsactiviteiten.pdf

²² https://www.gemmaonline.nl/images/gemmaonline/b/b7/Gegevenslandschap_-_Logging_van_verwerking_van_gegevens.pdf

²³ <https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

2.3. Integratiefuncties

De integratiefuncties bieden een combinatie van afspraken, standaarden en voorzieningen die betrekking hebben op het veilig kunnen uitwisselen van gegevens tussen organisaties. Denk hierbij aan functies voor het vindbaar maken van diensten, fysieke netwerken voor het verbinden van dienstverleners aan dienstverleners, functies voor de beveiliging en monitoring van netwerkverbindingen, en de uitwisseling van gegevens over deze verbindingen.



2.3.1. Netwerk

Diensten worden naar burgers en bedrijven en gemeenten en ketenpartners ontsloten via een netwerkinfrastructuur. Afhankelijk van de diensten die geboden worden is dit een privaat of een openbaar netwerk. Netwerken die gebruikt kunnen worden voor het benaderen van diensten zijn onder andere Internet en Diginetwerk koppelnetwerken zoals GGI-Netwerk. Door burgers en bedrijven zal met name gebruik worden gemaakt van internet voor het benaderen van de gemeentelijke diensten. Door gemeenten en ketenpartners kan ook gebruik worden gemaakt van Diginetwerk-koppelnetwerken. De keuze voor een netwerk is mede afhankelijk van het betrouwbaarheidsniveau van de dienst die wordt afgenomen. Het betrouwbaarheidsniveau van een dienst wordt bepaald door de dienstenaanbieder en is onder andere afhankelijk van de gevoeligheid en integriteit van de gegevens die via de dienst worden verwerkt.

Diensten die gesloten data verwerken zullen veelal een betrouwbaarheidsniveau kennen wat uitwisseling via een beveiligd netwerk vereist. Diensten die open data verwerken kennen vanuit het oogpunt van gevoeligheid van gegevens een laag betrouwbaarheidsniveau. Deze diensten kunnen aan externe afnemers beschikbaar worden gesteld via een open netwerk zoals Internet. Indien een afnemer echter hoge eisen stelt aan de integriteit van de open gegevens, en zeker wil weten dat gegevens tijdens transport niet gewijzigd zijn dan kan door de afnemer gekozen worden voor transport via een veiliger netwerk zoals een Diginetwerk-koppelnetwerk. De aanbieder van de dienst moet in het laatste geval wel ondersteuning bieden voor het leveren van de dienst via een beveiligd netwerk.

2.3.2. Netwerkbeveiliging

Het beveiligen van communicatienetwerken is onderdeel van de activiteiten die horen bij informatiebeveiliging. Informatiebeveiliging omvat het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit of vertrouwelijkheid en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Om de digitale infrastructuur in de moderne informatiemaatschappij effectief te beveiligen, is het inzetten van de 'klassieke' preventieve middelen zoals firewalls, antivirus, mail filtering, indringer detectiesystemen, etc. alleen niet meer voldoende. Geldende wet- en regelgeving vormen belangrijke drijfveren voor het nemen van

aanvullende maatregelen, zoals continue monitoring en analyse van acties en gedrag op de digitale infrastructuur, die helpen om voldoende weerbaar te zijn tegen dreigende inbreuken op de informatieveiligheid.

De functie 'Netwerkbeveiliging' geeft invulling aan de continue monitoring en analyse van het dataverkeer over het netwerk, en de daaraan gekoppelde signaleringsfuncties. Via het GGI-Veilig-portfolio kan invulling worden gegeven aan de preventieve als detectieve maatregelen op het gebied van netwerkbeveiliging.

2.3.3. Verbinden

Een essentieel onderdeel van de integratiefunctie is de verbindingfunctie. Belangrijkste verantwoordelijkheid van de verbindingfunctie is het tot stand brengen van een veilige verbinding tussen de aanbieder- en afnemer van de dienst zodat een afnemer op een veilige wijze de diensten van een aanbieder kan aanroepen.

Deze functie maakt gebruik van de dienstencatalogusfunctie om te bepalen waar een aanbieder van een dienst zich bevindt. Vervolgens maakt de functie voor het opbouwen van de verbinding tussen aanbieder en afnemer optioneel gebruik van client- en/of server certificaten (eenweg of tweeweg TLS). Voor het transport van de gegevens tussen de aanbieder en de afnemer wordt gebruik gemaakt van de netwerkfunctie.

Door VNG Realisatie wordt vanuit Common Ground gewerkt aan een stelsel van voorzieningen waarmee de verbindingfunctie kan worden ingevuld voor informatiesystemen die gebaseerd zijn op de architectuur van het GEMMA Gegevenslandschap. Deze verzameling van voorzieningen (het NLX-stelsel²⁴) is laagdrempelig voor ontwikkelaars, en voldoet aan de eisen die vanuit onder andere de Baseline Informatiebeveiliging Overheid (BIO) en privacywetgeving (AVG) gesteld worden. Gemeenten zijn echter vrij om voor de verbindingfunctie andere voorzieningen te gebruiken.

2.3.4. Dienstencatalogus

Het volledige dienstenaanbod dat beschikbaar is voor dienstenaanbieders is vastgelegd in dienstencatalogi. In deze catalogi worden de diensten vastgelegd die door dienstenaanbieders worden aangeboden voor gebruik. De diensten die een dienstenaanbieder aanbiedt, worden gepubliceerd en ontsloten via een dienstencatalogus. Diensten worden via REST/JSON- en, indien nodig SOAP/XML-, interfaces beschikbaar gesteld en worden in het geval van REST/JSON APIs conform de aanbevelingen uit de landelijke API-strategie beschreven volgens de OAS 3.x-specificatiestandaard. Diensten die een REST/JSON interface kennen conformeren zich aan de standaarden die hier landelijk voor gelden.²⁵

Dienstencatalogi zijn gericht op ontwikkelaars en bieden informatie over beschikbare diensten, en de vereisten voor het gebruik van de dienst. Een dienstencatalogus kan de volgende diensten aan ontwikkelaars bieden:

- Overzicht van diensten (APIs)
- API life-cycle informatie
- Criteria voor gebruik (API key, PKI, ..)
- API-documentatie

²⁴ <https://commonground.nl/file/download/54476629/Common%20Ground%20-%20NLX.pdf>

²⁵ <https://docs.geostandaarden.nl/api/API-Strategie/>

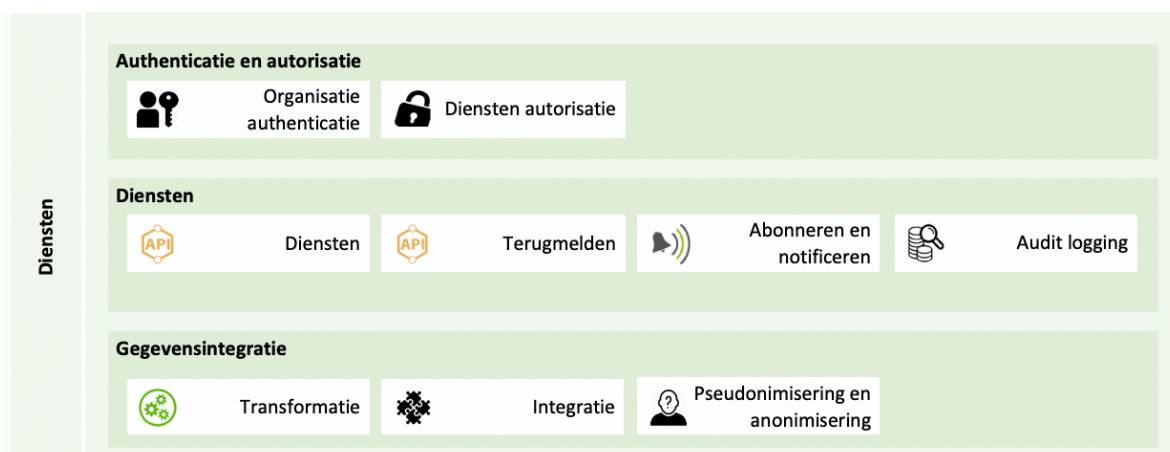
- Test- / uitprobeerfaciliteit

Een dienstencatalogus heeft enkel design-time een functie. Op run-time-niveau, dus tijdens de uitvoering van processen, wordt de dienstencatalogus niet gebruikt. De centrale dienstencatalogus vormt dus geen 'single point of failure' in de communicatie tussen dienstenafnemer en dienstenaanbieder.

Het GEMMA Gegevenslandschap schrijft geen specifieke dienstencatalogus voor, maar het inrichten van een centrale dienstencatalogus waarin alle APIs die door de overheid worden aangeboden, heeft vanuit het oogpunt van beperken van complexiteit de voorkeur.²⁶ Ook het NLX-stelsel, dat wordt ontwikkeld onder regie van VNG Realisatie, omvat een dienstencatalogusvoorziening. Op het NLX-stelsel aangesloten organisaties publiceren hierin hun diensten.

2.4. Diensten

De dienstenlaag van het GEMMA Gegevenslandschap bevat de diensten die nodig zijn voor onder andere autorisatie en authenticatie van afnemers, het leveren van gegevens, en het kunnen afleggen van verantwoording over welke diensten door wie gebruikt zijn.



2.4.1. Organisatie authenticatie

Een dienstenaanbieder stelt diensten ter beschikking aan dienstenafnemers. Het is van belang dat bij het gebruik van een dienst onomstotelijk vaststaat wat de identiteit van de dienstenafnemer is. Het leveren van een dienst aan een verkeerde dienstenafnemer zou immers kunnen leiden tot een datalek, misbruik van gegevens en potentieel schade voor inwoners, ondernemers of gemeente.

²⁶ In 2019 is het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met de Vereniging van Nederlandse Gemeenten / VNG Realisatie een initiatief gestart om een wegwijzer naar de APIs die (semi-)overheidsorganisaties in Nederland aanbieden te ontwikkelen (developer.overheid.nl).

Binnen de overheid wordt voor de identificatie van organisaties gebruik gemaakt van PKI-overheid-certificaten. Het PKI-overheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort. Er zijn twee soorten PKI-overheid-certificaten; Een PKI-overheid persoonsgebonden certificaat wat gebruikt wordt om een bepaalde persoon de mogelijkheid wilt geven elektronische (internet-)transacties te beveiligen en een PKI-overheid-servicescertificaat wat is gebonden aan een organisatie en wordt uitgegeven aan apparaten of servers, of groepen individuen. Het PKI-overheid-servicescertificaat wordt gebruikt om de communicatie te beveiligen tussen dienstenaanbieders en dienstenafnemers.

Uitgangspunt in het gegevenslandschap is dat voor de communicatie tussen dienstenaanbieders en dienstenafnemers gebruik wordt gemaakt van PKI-overheid services-certificaten voor zowel de aanbieder als de afnemer.

2.4.2. Diensten autorisatie

Binnen het gegevenslandschap wordt het principe van gedelegeerde autorisatie gebruikt. Als een dienstenafnemer gegevens nodig heeft van een dienstenaanbieder, is het uitgangspunt dat de dienstenaanbieder deze aanvraag niet opnieuw autoriseert op het niveau van de identiteit van de eindgebruiker, maar in plaats daarvan de autorisatie uitvoert op het niveau van de identiteit van de aanroepende dienstenaanbieder. De dienstenaanbieder autoriseert dus haar diensten op het niveau van een organisatie. Er is hierbij sprake van de aggregatie van identiteit van een specifiek niveau (bijvoorbeeld een gemeentelijke professional of burger) naar een generiek niveau (de gemeente). De autorisatie wordt afgeleid vanuit afspraken over de uitwisseling van gegevens die tussen de dienstenaanbieder en dienstenafnemer zijn gemaakt. Deze afspraken, ook wel gegevensleveringsovereenkomsten (GLO) genoemd, dienen door de dienstenaanbieder vertaald te worden naar autorisatieprofielen. Per organisatie kan in een autorisatieprofiel worden vastgelegd voor welke specifieke diensten een geauthentiseerde dienstenafnemer is geautoriseerd. Alleen de diensten waarvoor de dienstenafnemer is geautoriseerd kunnen door de dienstenafnemer worden gebruikt.

2.4.3. Diensten

Een dienstenaanbieder biedt via diensten toegang tot de gegevens die door de dienstenaanbieder verwerkt worden. Deze diensten hebben meestal de vorm van een webservice met bij voorkeur een RESTful API interface. Indien een dienst de vorm REST/JSON heeft, dan moet deze zich conformeren aan de landelijke standaarden die hiervoor gelden.²⁷

Er zijn verschillende soorten diensten te onderscheiden die door een dienstenaanbieder kunnen worden geboden. De landelijke API-strategie onderkent de volgende typen APIs:

- Systeemdiensten; dit type dienst werkt op het niveau van de databron en is gericht zijn op het ontsluiten en bijwerken van de gegevensverzameling die wordt bijgehouden. Het gaat hier dus met name om de zogenaamde CRUD-functionaliteit²⁸ voor het aanmaken, lezen, wijzigen en verwijderen van gegevens. Een voorbeeld van een systeemdienst is een dienst waarmee een klant wordt toegevoegd aan een klantenregister;

²⁷ <https://docs.geostandaarden.nl/api/API-Strategie/>

²⁸ <https://nl.wikipedia.org/wiki/CRUD>

- Procesdiensten; deze diensten orkestreren één of meerdere systeemdiensten door deze aan te roepen en de resultaten gebundeld terug te geven aan de aanroepende partij. Procesdiensten zijn ingericht op het beantwoorden van een specifieke vraag van een afnemer.
- Gemaks- of ervaringsdiensten; dit soort diensten beantwoorden één specifieke gebruikersvraag. Een voorbeeld van een dergelijke dienst is een dienst die op basis van een BSN als resultaat geeft of de betreffende persoon ouder is dan 18 jaar. Deze diensten hebben als voordeel dat ze het mogelijk maken om proportioneel en subsidiair gegevens te verstrekken. Een drankwinkel heeft bijvoorbeeld de wettelijke verantwoordelijkheid om na te gaan of iemand ouder dan 18 jaar is voordat aan diegene alcoholhoudende drank mag worden verkocht. Een simpel 'ja, ouder dan 18 jaar' of 'nee, jonger dan 18 jaar' voldoet om aan deze verplichting te voldoen. De betreffende winkelier hoeft dus niet de actuele leeftijd of de geboortedatum te kennen.

Systeemdiensten moeten door alle dienstenaanbieders worden geboden. Dit zijn immers de elementaire diensten waarmee een gegevensverzameling onderhouden wordt. Of een dienstenaanbieder ook proces- en gemaksdiensten aanbiedt, is afhankelijk van de vraag van de afnemers. Deze laatste twee soorten diensten worden namelijk volledig afgestemd op de behoefte van de afnemers.

Een belangrijk uitgangspunt is dat een leverancier van diensten zelf ook gebruikmaakt van de aangeboden diensten, óók om 'eigen' gegevens te benaderen. Een leverancier die een bronsysteem en processysteem levert, mag voor zichzelf dus geen aparte set van APIs gebruiken voor toegang tot de brongegevens. Door deze '*eat your own dogfood*'-benadering²⁹ wordt gewaarborgd dat diensten die worden geboden exact doen wat ze moeten doen op een efficiënte en effectieve manier. Het voorkomt dat meerdere implementaties van vergelijkbare functionaliteit ontstaan met mogelijke functionele of technische verschillen, en dat een leverancier bij het benaderen van gegevens een voordeel heeft ten opzichte van derden.

2.4.4. Terugmelden

Voor ieder bronregister in het GEMMA Gegevenslandschap geldt dat de bronhouder afnemers van gegevens in staat moet stellen om twijfels over de correctheid van gegevens door te geven. Deze functionaliteit is vergelijkbaar met de terugmeld mogelijkheden die de landelijke basisregistraties bieden. De verplichting om deze functionaliteit te bieden komt enerzijds voort uit de (AVG-)rechten van burgers ten aanzien van het corrigeren van de 'eigen' gegevens, en anderzijds het streven naar een zo hoog mogelijke kwaliteit en actualiteit van gegevens. Hoewel het wettelijke recht op terugmelden vanuit de AVG (correctierecht) alleen geldt voor persoonsgegevens en gegevens die naar een persoon herleidbaar zijn, is vanuit het oogpunt van de verbetering van de kwaliteit van gegevens in het GEMMA Gegevenslandschap gekozen om ieder register de verplichting op te leggen om terugmelden te implementeren.

Functionaliteit voor terugmelden kan door de dienstenaanbieder gerealiseerd worden door een combinatie van APIs waarmee een terugmelding kan worden doorgegeven, en notificatiefunctionaliteit om de indiener van de terugmelding op de hoogte te stellen dat de melding is afgehandeld. De melder kan dan via een bevragingsdienst

²⁹ https://en.wikipedia.org/wiki/Eating_your_own_dog_food

de uitkomst van de afhandeling inzien. De bronhouder dient uiteraard processen in te richten die terugmeldingen signaleren, en acties uit te zetten voor het afhandelen van de terugmeldingen.

Er is op dit moment geen standaard gedefinieerd voor het terugmelden op registers anders dan basisregistraties. Het ontwikkelen van zo'n standaard is naar verwachting wel wenselijk.

2.4.5. Abonneren en notificeren

Uitgangspunt van het GEMMA Gegevenslandschap is dat gegevens worden opgehaald bij de bron op het moment dat ze nodig zijn. Op het moment dat gegevens in een bron wijzigen, kan het nodig zijn om afnemers die gebruik maken van die gegevens hiervan op de hoogte te stellen omdat een wijziging van gegevens vaak kan leiden tot het starten van een proces. Op dit moment leveren basisregistraties voor dit doel meestal 'was-wordt'-mutatiebestanden aan afnemers. De gegevens uit deze bestanden worden verwerkt in de gemeentelijke administraties, en gebruikt om gebeurtenissen te genereren waarmee interne gemeentelijke processen worden gevoed. Bij het rechtstreeks bij de bron bevragen, beogen we ook het stoppen met het ontvangen en verwerken van 'was-wordt'-mutatiebestanden. We verlangen immers van gemeenten dat gegevens bij de bron worden bevraagd, en (dus) dat ze stoppen met het bijhouden van eigen schaduwregistraties. Dit betekent ook dat gemeenten niet langer in staat zijn gebeurtenissen die bij bronregisters hebben plaatsgevonden van 'was-wordt'-bestanden af te leiden.

Het versturen van dergelijke gebeurtenissen is in de GEMMA Gegevenslandschap-architectuur de verantwoordelijkheid van het bronregister. In de informatiearchitectuur wordt dit een 'event driven architecture' (EDA) genoemd. Een set van landelijke afspraken, standaarden en voorzieningen is essentieel voor het slagen van een overheidsbreed gegevenslandschap. Dit voorstel gaat over de eerste stappen om tot die landelijke functionaliteit te komen.

Dienstenaanbieders moeten afnemers daarom de mogelijkheid bieden om abonnementen af te sluiten op gebeurtenissen in een gegevensbron. Afnemers kunnen bij de bron aangeven op welke gebeurtenissen ze een abonnement willen afsluiten. De dienstenaanbieder zorgt er daarbij voor dat de afnemer alleen abonnementen kan afsluiten voor gebeurtenissen of gegevens waarvoor de afnemer geautoriseerd is.

Op het moment dat er een wijziging optreedt in het bronregister zal de dienstenaanbieder alle geabonneerden een notificatiebericht sturen. Dit notificatiebericht bevat sleutelgegevens van het object waarover de notificatie gaat, en de context van de notificatie (wat is er gebeurd en waarom). Verder worden geen inhoudelijke gegevens opgenomen in de notificatie. De ontvanger van de notificatie kan aan de hand van de inhoud daarvan bepalen of, en zo ja, welke interne processen opgestart moeten worden, en kan, indien gewenst, met de sleutelgegevens aanvullende detailgegevens van het object ophalen bij het bronregister.

Een voorbeeld van het bovenstaande is een afnemer die een abonnement afsluit op de persoonsgegevens van een bepaald BSN. Op het moment dat in de persoonsregistratie een wijziging optreedt, bijvoorbeeld nadat de persoon verhuist, zal de persoonsregistratie een notificatie over deze wijziging sturen naar de geabonneerde afnemers. De afnemer kan zien dat de notificatie betrekking heeft op een wijziging van de persoonsgegevens van een bepaald BSN, en dat de reden voor die wijziging een verhuizing is. De afnemer kan op basis van deze informatie besluiten om wel of geen actie te ondernemen.

2.4.6. Audit logging

Alle aanroepen van diensten, of deze nu succesvol zijn geweest of niet, moeten ten behoeve van transparantie- en verantwoordingsdoeleinden door de dienstenaanbieder in logbestanden worden vastgelegd. In de logbestanden wordt naast de datum en tijd van de aanroep een aantal meta-attributen vastgelegd. Deze attributen omvatten onder andere de identificatie van de organisatie die de dienst heeft aangeroepen (OIN³⁰), de doelbindingsclaim en een uniek log-ID waarmee de aanroep herleid kan worden naar de logging van de dienstenafnemer. Door de logging van de dienstenaanbieder en -afnemer te combineren kan een sluitende audit-log worden samengesteld. Deze audit-log kan worden gebruikt om vast te stellen of de verwerking van gegevens door de dienstenafnemer rechtmatig was .

2.4.7. Transformatie

Bij het leveren van diensten kan het nodig zijn om gegevens te transformeren alvorens ze aan een afnemer te leveren. Dergelijke transformaties kunnen eenvoudig zijn (bijvoorbeeld het omzetten van een datumformaat yyyymmdd naar dd-mm-yyyy), maar meer complexe transformaties, zoals een conversie van coördinaten naar een ander geodetisch coördinatensysteem, zijn ook mogelijk.

Omdat transformatie het ingewikkelder maakt om de oorsprong van gegevens te herleiden, moet het transformeren van gegevens zoveel mogelijk voorkomen worden. Als alle bronregisters vanuit een gestandaardiseerd stelsel van informatiemodellen zouden werken zou transformatiefunctie minder nodig zijn. Gemeenten hebben echter te maken met keten- en netwerkpartijen die eigen afspraken en standaarden volgen. Transformatie van gegevens in verband met niet op elkaar aansluitende standaarden is daarom in sommige gevallen niet te voorkomen.

2.4.8. Integratie

Diensten kunnen werken op het niveau van de databron, gericht op het ontsluiten en bijwerken van de gegevensverzameling die door de dienstenaanbieder wordt bijgehouden (System APIs), of gericht op het beantwoorden van één specifieke gebruikersvraag. Deze laatste categorie van diensten moeten vaak gegevens uit databronnen combineren om de gebruikersvraag te beantwoorden.

Stel bijvoorbeeld dat de Basisregistratie Adressen en Gebouwen (BAG) wordt bevraagd. De vraag “Wat is het volledige adres bij deze postcode?” is alleen te beantwoorden door intern bij een Verblijfsobject uit de BAG de ‘Openbare Ruimte naam’, ‘Nummeraanduiding’ en ‘Woonplaats’ op te vragen en te combineren tot één adressering. Dit vraagt om meerdere aanroepen van System APIs en het combineren van de antwoorden om deze gangbare (maar complexe) vraag in één aanroep te beantwoorden.

Integratie wordt binnen diensten toegepast om de complexiteit voor een zo groot mogelijk deel van de afnemers te verbergen en de toepasbaarheid van een dienst zo groot mogelijk te maken.

³⁰ <https://www.logius.nl/diensten/oin>

2.4.9. Pseudonimisering en anonimisering

Om bijvoorbeeld analysetoepassingen mogelijk te maken, en tegelijkertijd te voldoen aan relevante wetgeving, kan het nodig zijn om gegevens te pseudonimiseren³¹. Met deze techniek worden de identificeerbare elementen van een van een dataset, zoals een BSN en een persoonsnaam, verwijderd en omgezet naar een betekenisloos nummer. In zo'n proces worden met behulp van een bepaald algoritme identificerende gegevens vervangen door versleutelde gegevens (het pseudoniem). Pseudonimisering kan dus gezien worden als een beveiligingsmaatregel. Het vermindert het privacyrisico van de betrokkenen en het bewerkingsrisico voor de organisatie(s).

Vanuit de privacywetgeving is het pseudonimiseren van gegevens in sommige gevallen verplicht. In de handreiking "Stroomschema pseudonimisering (AVG)³²" is een stappenplan opgenomen dat gebruikt kan worden om te toetsen of het gebruik van gepseudonimiseerde gegevens toegestaan is. Omdat het algoritme voor een persoon altijd hetzelfde pseudoniem bepaalt, is het mogelijk gegevens over één persoon uit verschillende bronnen te combineren, of die gegevens terug te herleiden naar BSN of persoonsnaam. Hierdoor blijven gepseudonimiseerde gegevens persoonsgegevens en moeten ze conform de eisen uit de privacywetgeving behandeld worden.

Ten behoeve van bijvoorbeeld de publicatie van open data kan het nodig zijn om gegevens te anonimiseren. Net als bij pseudonimisering worden identificerende gegevens hierbij middels een algoritme vervangen door versleutelde gegevens. Het verschil met pseudonimisering is dat bovenstaand proces bij anonimisering onomkeerbaar is: het is dus onmogelijk om geanonimiseerde gegevens terug te herleiden naar de oorspronkelijke identiteit van de persoon waarbij ze hoorden. Geanonimiseerde gegevens zijn daarom geen persoonsgegevens meer, en dus is de AVG niet van toepassing op deze gegevens.

Belangrijke randvoorwaarde bij anonimiseren is dat alle herleidbare persoonsgegevens gemaskeerd worden. Het anonimiseren moet daarnaast geautomatiseerd uitgevoerd worden of door personen die geautoriseerd zijn om de te anonimiseren gegevens in te zien: vóór het voltooien van het anonimiseringsproces is immers nog gewoon sprake van persoonsgegevens, waarvoor de AVG-regels van toepassing zijn.

³¹ <https://nl.wikipedia.org/wiki/Pseudonimiseren>

³² <https://www.rijksoverheid.nl/documenten/richtlijnen/2018/02/15/stroomschema-pseudonimisering-avg>

2.5. Gegevensbronnen

De gegevensbronnen van het GEMMA Gegevenslandschap bieden de diensten die nodig zijn voor het compliant aan wet- en regelgeving kunnen bijhouden en ontsluiten van gegevens.



2.5.1. Bijhouding gegevens

Uitgangspunt van het GEMMA Gegevenslandschap is dat registers qua syntax en samenhang door de bronhouder gestandaardiseerd zijn. Onderdeel van deze standaardisatie is het beschrijven van de syntax en samenhang van gegevens in een informatiemodel. Het informatiemodel vormt de formele beschrijving van alle informatie die van belang is binnen een gegeven domein, en beschrijft het domein in termen van objecten, attributen daarvan en relaties daartussen.

Om alle informatiemodellen in Nederland beter op elkaar aan te laten sluiten hebben VNG Realisatie, Kadaster en Geonovum gezamenlijk een metamodel ontwikkeld voor informatiemodellering: het Metamodel voor Informatiemodellen (MIM)³³. Het MIM vormt een gemeenschappelijk vertrekpunt voor het maken van informatiemodellen, waarin duidelijke afspraken over het vastleggen van gegevensspecificaties op verschillende niveaus zijn beschreven. Bijzonder aan het model is dat de afspraken bestuurslaagoverschrijdend gelden.

Gemeentelijke gegevens worden onder regie van gemeenten gestandaardiseerd via informatiemodellen. Het gaat hierbij om sectorale of domeinspecifieke gegevens en gemeentelijke kerngegevens. Daar waar landelijk vastgestelde catalogi bestaan ten aanzien van de gegevens worden deze gevolgd. Een voorbeeld van een dergelijke catalogus is het is Suwi gegevensregister (SGR)³⁴. Daarnaast kan het ook gaan om taakspecifieke gegevens die voor verschillende doelen gebruikt moeten kunnen worden. Bijvoorbeeld om ze via verschillende interactievoorzieningen aan te bieden.

³³ http://www.gemmaonline.nl/images/gemmaonline/6/66/Metamodel_informatiemodellen_KING_Kadaster.pdf

³⁴ <https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr/>

2.5.2. Historie en metadatering gegevens

Bronregisters binnen het GEMMA Gegevenslandschap moeten voldoen aan de DUTO kwaliteitscriteria: informatieobjecten moeten vindbaar, beschikbaar, leesbaar (en bruikbaar), interpreteerbaar en betrouwbaar (authentiek en integer) zijn. Het is de verantwoordelijkheid van de dienstenaanbieder om te waarborgen dat informatieobjecten (gegevensobjecten en documenten) waarvoor de aanbieder het bronregister beheert, aan deze eisen voldoen. Om dit mogelijk te maken is het uitgangspunt dat informatieobjecten die in een bronregister worden opgeslagen altijd voorzien moeten zijn van een minimale set van verplichte metagegevens (compliance metadata). Dit is alleen mogelijk door toepassing van by-design principes: metadata worden zoveel mogelijk automatisch gecreëerd en geüpdatet naar aanleiding van gebruik in processen en/of diensten. Zo kan worden voldaan aan de eisen van de Archiefwet, AVG, Wet Openbaarheid van Bestuur (WOB), Wet hergebruik van overheidsinformatie (Who) en de Wet open overheid (Woo).

Daarnaast is de vastlegging van de historie van brongegevens ook een belangrijk aspect bij de opslag van gegevens. Deze historie kent twee 'werkelijkheden': formele historie (dat wat wijzigt in de registratie), en materiële historie (dat wat wijzigt in de werkelijkheid). Het is voor veel afnemers van belang dat iedere relevante toestandsverandering van een object in het register, zowel formeel als materieel, bekend is. Bij voorkeur wordt daarbij ook de aard van plaatsgevonden mutaties vastgelegd. Deze manier van registratie maakt bevraging op peildatum mogelijk, wat voor veel toepassingen en afnemers noodzakelijk is. Waar die noodzaak bestaat, en formele- en materiële historie niet in het register worden bijgehouden, zal bij afnemers de noodzaak blijven bestaan om gegevens lokaal, dus redundant, bij te houden. Het bijhouden van historie is niet voor alle bronregisters van belang. Daar waar het functioneel bijhouden van historie niet vereist is, hoeft geen historie te worden vastgelegd.

2.5.3. Protocollering

Iedere vorm van administratie kent methoden om de juistheid van een administratieve handeling te waarborgen. Een onjuiste handeling die niet wordt opgemerkt, kan leiden tot fouten in de administratie. Daardoor kunnen de belangen van degenen die gegevens uit die administratie gebruiken, ernstig worden geschaad. Het is daarom van belang dat nagegaan kan worden of uitgevoerde administratieve handelingen juist zijn uitgevoerd. In de Wet Basisregistratie Personen (BRP) is voorgeschreven dat alle handelingen van het systeem dat de Wet implementeert, in beginsel door het systeem zelf moeten worden vastgelegd. Deze vastlegging wordt 'protocolleren' genoemd. In de protocollering wordt ook vastgelegd welke gegevens uit de registratie wanneer, door wie, over wie en aan wie zijn verstrekt.

Het op deze manier vastleggen van administratieve handelingen en ook gegevensverstrekkingen heeft twee functies. Ten eerste kan uit de protocollen worden afgeleid of het systeem de verstrekking juist heeft uitgevoerd. Ten tweede is de vastlegging van een gegevensverstrekking een belangrijk bestanddeel in het stelsel tot bescherming van de persoonlijke levenssfeer van de burger. Het is het sluitstuk. Achteraf kan op basis hiervan immers worden herleid of de gegevensverstrekking rechtmatig heeft plaatsgevonden: dit wordt de privacyfunctie genoemd.

Hoewel de reikwijdte van begrip protocollering oorspronkelijk beperkt is tot de Wet Basisregistratie Personen, zou iedere bronregistratie protocollering moeten bijhouden, zodat op detailniveau verantwoording kan worden afgelegd over uitgevoerde administratieve handelingen.